# Information Commissioner's Office

## Internal Audit 2013-14: IT Service Management review

Last updated 28 May 2014

| Distribution | | Timetable | |
|---|---|---|---|
| For action | Director of Corporate Services | Fieldwork completed | 12 February 2014 |
| For information | Head of IT | Draft report issued | 26 February 2014 |
| For information | Audit Committee | Management feedback | 20 March 2014 |
| | | Management comments | 27 May 2014 |
| | | Final report issued | 28 May 2014 |

# 1 Executive Summary

## 1.1 Background

In 2013 the ICO established a new set of IT service contracts with a number of new suppliers, replacing a single contract with Capita. Northgate were awarded the two main contracts: Hosting & Infrastructure and Applications & Desktops. As a result, Northgate runs the Service Desk for the ICO, receiving calls from members of staff relating to any incidents with IT.

Northgate have also sub-contracted some services to a number of specialist providers:

**Eduserve:** host and develop the public facing Internet web site used by the ICO's customers and other stakeholders

**Frontline:** support for the business intelligence software (Cognos).

**Kainos:** software development and support for the ICO's case management system.

**Pinnacle:** installation, service and support on the telephone system.

SCC provides advice and consultancy to the ICO on information security related matters. SCC also provide a purchasing service for software licences and hardware, plus any related advice to the ICO. There is an indirect relationship between Northgate and SCC, where Northgate may require security advice and keep ICO appraised of security issues.

The ICO uses Danwood to provide support, maintenance and supply of printing facilities. The ICO also uses FDM to provide bulk printing services, for publicly available printed material. FDM deals with the ICO directly and has no other interaction with other suppliers.

The ICO has had to adapt to managing multiple suppliers rather than a single supplier, as before with Capita. As part of the new arrangements, the IT department will take ultimate responsibility for faults, but the recording and day to day management of faults and assigning responsibility to the appropriate supplier of the relevant service is part of the Service Desk, delivered by Northgate. Where ownership of the incident is not clear, the IT department is expected to take the lead to ensure incidents are resolved, typically by facilitating resolution with multiple suppliers.

## 1.2 Scope

Our review involved an assessment of the following risks:

- Service delivery that does not meet ICO requirements.
- Service levels that are unclear or poorly defined lead to misalignment of delivery to user expectations.
- A lack of clear understanding of what is included in the service delivery leading to disputes over ownership or changes that are not appropriately managed that prevent service disruption.
- An inefficient incident management service extends disruption or common faults are not identified to prevent future incidents.

Further details on responsibilities, approach and scope are included in Appendix A.

## 1.3 Overall assessment

We have made an overall assessment of our findings as:

| Overall assessment | |
|---|---|
| Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which require the attention of management to resolve and report on progress in line with current follow up processes. | **Amber** |

Please refer to appendix B for further information regarding our overall assessment and audit finding ratings.

## 1.4 Key findings

| Risk / Process | High | Medium | Low | Imp |
|---|---|---|---|---|
| Service delivery not meeting ICO needs | - | 1 | - | 1 |
| Unclear service definition | - | - | 1 | - |
| Lack of clarity over what is included in service delivery | - | 4 | - | - |
| Ineffective incident management | - | - | 2 | - |
| **Total** | **-** | **5** | **3** | **1** |

The following findings were rated as medium priority:

- Problems have not, until recently, been managed proactively by the supplier to ensure sufficient resources are being deployed to resolve issues in a timely manner. In addition, users have not received feedback on the status and progress of Problems reported.
- A baseline of the ICO IT systems performance was not established prior to Northgate assuming responsibility for maintenance and support. This makes it more difficult to properly investigate Incidents or Problems, since the level of "normal" performance is not known. Northgate and the ICO are working collaboratively on any immediate issues, and on identifying short term infrastructure investment needs, however a longer term capacity plan is also needed for the future, on the basis of which expected performance levels can be established..
- Provision of an IT Disaster Recovery service is part of the Northgate contract but has yet to be tested. A test was planned in 2013 but was postponed because additional work was required to improve security of the Disaster Recovery equipment. Without a tested recovery plan, the ICO could suffer extended system disruption due to a recovery plan that does not work as expected.
- The transition from Capita includes identifying all the items that are now covered by Northgate and their sub-contractors. The details of such items should be kept in a Configuration Management Database, which allows all parties to establish what is included in the contract (in terms of hardware, software, infrastructure etc) at a detailed level. However such a database has not yet been established by Northgate.
- ICO is responsible for establishing software licence compliance but due to long term illness this is not currently being actively managed. Whilst only Northgate can install software, the ICO is responsible for monitoring compliance, establishing licence agreements with vendors and procuring additional licences as required.

Further details of our findings and recommendations are provided in Section 2.

## 1.5 Areas of control in line with expectations

- The ICO has established a new function within IT, to manage and oversee change management of IT systems. The ICO has taken the lead to manage, approve and monitor changes within the IT estate.
- The ICO has now established a framework of contacts that will expire at different times, preventing the significant resources and effort required to tender and let new contracts.
- Contacts have been established defining the details of services provided and related service credits for poor performance.
- Engagement from senior management and management of the IT contracts to ensure appropriate management involvement in supplier management, from business as usual activity on a day to day basis as well as formal quarterly meetings between senior ICO management and suppliers.

## 1.6 Elsewhere in the sector

We detail below other ways of working and commonly occurring issues that we have experienced during similar types of reviews for other public bodies. The following does not necessarily purport to be good practice but is included for your information and consideration.

- Although a structure of service credits is often used to manage performance, many organisations also aim to reward strong outcomes as well, in a collaborative approach to sharing risk and reward.

## 1.7 Acknowledgement

We would like to take this opportunity to thank the staff involved for their co-operation during this internal audit.

# 2 Detailed Findings

## 2.1 Service delivery not meeting ICO needs

| 1. | Medium | Managing problems |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| The IT Infrastructure Library (ITIL) is a best practice framework for managing IT services. ITIL defines Problems as the cause of one or more incidents. Problem management is a recognised process within ITIL and has been adopted by ICO and Northgate. Problems are being referred to Northgate for investigation but, until recently, were not being actively managed.<br><br>The IT Service Manager has identified that whilst problems were being reported to Northgate and being covered as part of the monthly meetings, sufficient progress was not being made.<br><br>Further discussion with the IT Service Manager also established that Problems are not currently subject to any defined measures of quality of service to ensure appropriate resources are in place to manage Problems to a satisfactory conclusion, other than by review during weekly and monthly service meetings. Northgate are focused on minimising service credits, the penalty imposed by the ICO on not delivering services to an agreed standard and quality. Currently, Problems – or failure to manage them - are not subject to service credits.<br><br>During discussions with end users, there is no visibility of the progress being made with Problems that have been reported. | The IT Service Manager should establish a mechanism whereby performance by suppliers in addressing problems can be monitored, the supplier held to account against these measures. Performance in this respect would normally fall into the service credits regime. | *Agreed action:* Since this review took place, the management, control and effectiveness of Problem Management (PM) has been raised with Northgate: Additional monitoring of PM has been put in place; There is now a monthly PM review meeting; Northgate produce a monthly PM report; PM has been added to the agenda for the monthly service meetings.<br><br>There is now clear evidence that problems are being investigated, solutions found and implemented, and the backlog of problems is being worked through.<br><br>No further controls are considered necessary. The inclusion of PM in the service credit regime has been noted for any new contract.<br><br>*Date Effective: 27 May 2014*<br><br>*Owner: Head of IT* |

| 1. | Medium | Managing problems |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| A lack of visibility of progress can lead to users not using the service as they should, and looking for alternatives to achieve satisfactory resolution. Such practices can hide the use of resources on an ad hoc basis, and reporting of performance around incident or problem resolution can be misleading, if all incidents or problems are not managed through a consistent process. | The IT Service Manager should ensure that users obtain feedback from the relevant supplier on resolution progress and on the status of Problems reported. | *Agreed action* An objective has been added this year for IT Service Delivery staff to improve communications with the business. Improvements are planned to the IT ICON pages to provide more updates and relevant information; IT staff has attended an 'improving communication' workshop (specifically aimed at producing effective brief communications).<br><br>*Date Effective: 27 May 2014*<br><br>*Owner: Head of IT* |

| 2. | Improvement | Clarity over IT Service Manager and Contract Manager roles |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| At the time of establishment of the new contracts to replace the Capita contract, the ICO had put in place the roles of IT Service Manager and Contract Manager. However, due to unforeseen circumstances, the Contract Manager had not been able to engage as expected on IT contract issues. The result is a prioritisation of Contract issues over some IT Service Delivery responsibilities, resulting in some parts of the IT Service Manager's role not being discharged. This is highlighted by the poor performance of suppliers in respect of problem management (see finding 1, above).<br><br>However, after the fieldwork of the review, Contract Manager was able to take a more active role in supporting of IT contract management and that the IT Service Manager's job description has been updated. The IT Service Manager has on-going responsibility for contract management but will be supported by the Contract Manager. | ICO to confirm that actions taken have addressed the responsibilities for contract management between the IT Service Manager and Contract Manager.<br><br>Note: The IT Contract Management review will be able to confirm the activities in place. | *Agreed action* No changes or additional controls considered necessary. Any actions will be picked up in the IT contract review.<br><br>*Date Effective: 27 May 2014*<br><br>*Owner: Head of IT* |

## 2.2 Service level definition unclear

| 3. | Low | Lack of a detailed Service Catalogue |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| The Service Catalogue is a definitive list of all IT services that an organisation uses or deploys for their customers' use. A Service Catalogues does exist but only at a high level. Northgate are responsible for establishing the Service Catalogue at the ICO but this remains an outstanding deliverable from the transition from Capita.<br><br>ITIL defines that the Service Catalogue documents all live services. A Service Catalogue should include details such as service level definition, service provider, service owner and such further information about the service and its "boundaries" as may be needed.<br><br>Without a comprehensive Service Catalogue in place, the ICO may have gaps regarding ownership over service provision, or may have services is required but currently not in place.<br><br>The Catalogue can also be used as the base from which service credits are applied. The service catalogue would also link to the Configuration Database referred to in finding 6, below. A comprehensive Service Catalogue provides a focal point for the IT Service Manager and the suppliers when discussing service provision, especially if the is doubt over an IT service or IT equipment and that it is part of the service.<br><br>We note that there is list of services in place as part of the contract but only at a high level: there are no details associated with each service. | IT Service Manager to ensure that a date for completion of the Service catalogue is agreed with Northgate. | *Agreed action*<br><br>Much of the service catalogue is already in place within the contract, although some details remain to be completed by Northgate. Since the Grant Thornton review, Northgate have made progress on completing transition activities – Target date to complete all actions, including the service catalogue, is the 9 July 2014 (the contract anniversary). Documentation is being quality checked and signed off by ICO Service Delivery Manager.<br><br>*Date Effective:* 9 July 2014<br><br>*Owner:* Head of IT |

## 2.3 Lack of clarity over what is included in service delivery

| 4. | Medium | Establish current IT systems performance |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| Northgate have assumed responsibility for taking over managing the ICO IT equipment from Capita. However, what has not been established is the baseline performance measures which define the starting level of acceptable performance from existing systems. Without a baseline, ICO may either demand a better performance than was in place, or conversely expect a lower level of performance without questioning it. If a better level of performance is demanded, Northgate may conclude that additional investment in technology or resources is required, which may mean the contract costing the ICO more.<br><br>Currently, Northgate and ICO are working cooperatively to resolve any immediate performance issues and neither party is relying upon historical performance as a benchmark.<br><br>A capacity plan is part of the Northgate contract but is not yet in place. A project is under way to identify any immediate (within the next 6 months) needs that require ICO to invest further in the current IT infrastructure. | The IT Service Manager to establish current baseline performance measures with Northgate to provide a common understanding of performance. The baseline assessment can be used to support the investigation of any Incident or Problem raised where performance(for example such as speed or availability) may the root cause.<br><br>As the service delivery matures both Northgate and ICO need to establish acceptable performance levels, and work on a capacity plan that allows for a considered and timely changes to the IT infrastructure to meet future needs.<br><br>The Head of IT to agree a timetable with Northgate for the establishment of an IT capacity plan and the frequency with which the plan should be updated in future. | *Agreed action* Baseline performance data was captured in the first four month of the contract. It should be noted that there are no general performance issues with the IT systems. Any performance issues arising from system changes have been quickly investigated and dealt with.<br><br>Next action to measure performance at the contract anniversary, 9 July 2014<br><br>*Date Effective:* 9 July 2014<br><br>*Owner:* Head of IT<br><br>*Agreed action* Capacity planning exercise to be undertaken after contract anniversary (9 July).<br><br>*Date Effective: 31 Aug 2014*<br><br>*Owner:* Head of IT |

## 5. Medium — Establish a test of Disaster Recovery Plans

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| ICO and Northgate were planning to test the IT Disaster Recovery Plan in 2013 but this was postponed at the request of ICO. Additional work was identified to improve the security of the Disaster Recovery systems.<br><br>Without a tested Disaster Recovery Plan, in the event of an incident requiring ICO to operate information systems from another location, the recovery may take longer than planned and extend the period of disruption. | IT Service Manager to agree a date to test the IT Disaster Recovery Plan, as quickly as possible. | *Agreed action A* DR test took place between 22 April and 2 May 2014.<br><br>*Date Effective: 2 May 2014*<br><br>*Owner:* Head of IT |

## 6. Medium — Lack of details for all items covered by the contract

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| As part of any IT services contract, a comprehensive list should be in place to allow suppliers and ICO to know what is in scope as part of the service provision and what is not. Northgate are in the process of establishing such a list but this has not been completed.<br><br>As part of the transition from Capita, a Configuration Management Database was to be put in place that lists all configurable items (such as IT services, IT equipment, software, buildings, people and documentation), as defined in ITIL. These configurable items provide the building blocks for managing services by providing details of each item and relationships with other items. A lack of detailed information can result in disputes as to whether an item is included in a service or not. A Service Desk that records any Incident or Problem and its resolution also depends upon the configuration information to ensure the authenticity of an event and to establish exactly what it relates to. | IT Service Manager should agree a timetable with Northgate to establish the Configuration Management Database. | *Agreed action* Northgate plan to capture CMDB information during June and hold this information in their Secure Management Enclave which is accessible to their support staff.<br><br>*Date Effective:* 30 June 2014<br><br>*Owner:* Head of IT |

| 7. | Medium | Software licence management |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| The ICO's responsibility in respect of licence management is to ensure sufficient licences are available when required, appropriate licence agreements are in place with software vendors and to procure additional licences as required. However, due to extended sick leave, this is currently not being actively managed. A lack of management over software licences could expose the ICO to users not being able to carry out their duties due to a lack of available software.<br><br>Only Northgate can install software and will only install software under instruction from the ICO. However, it is not clear who would be responsible for establishing whether the ICO is compliant with the licensing requirements of software usage, and whilst this has not created any particular issues since the new contracts have been in place, the matter should be resolved and responsibility established.<br><br>There is the potential of reputation damage if the ICO did not comply with software licence agreements. | The Head of IT to establish who will manage software licences and confirm their responsibilities. | *Agreed action* Licenses have been managed in the interim by the Head of IT. Review whether this function needs to be reassigned by end Q1 2014<br><br>*Date Effective:* 30 June 2014<br><br>*Owner:* Head of IT |

## 2.4 Ineffective incident management

| 8. | Low | Latest change control policy and procedures not approved and available to users |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| During our review, we reviewed a copy of the Change Control Policy and Change Procedures, but they were awaiting approval from management.<br><br>A lack of clarity over any policy or procedure could raise doubt over the documents validity and introduces doubt as to whether they should be followed. | Head of IT to ensure that the latest version of Change Control Policy and Change Control Procedure are approved by an appropriate management body and published so users have easy access. | *Agreed action* Policy has been agreed and published. No additional actions planned from this recommendation.<br><br>Note that in addition; the operation of the Change Control process is to be discussed at the annual Contract review meeting in July 2014 with the aim of harmonising the process across the two organisations.<br><br>*Date Effective:* 27 May 2014<br><br>*Owner:* Head of IT |

| 9. | Low | Authority to approve emergency changes |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| We reviewed the Change Management Policy - Technical Changes and it was unclear who had the authority to approve an emergency change.<br><br>The policy refers to "The Service Manager", "The Head of IT" or "An assigned deputy" have the authority to approve an emergency change. However, under the Roles and Responsibilities section, there is a body called the "Emergency Change Committee" which consists of one member of the Change Management Board and one other. An unclear change control policy could lead to an emergency change being introduced that could cause disruption to services if not appropriately approved.<br><br>We have seen elsewhere that at least two people should sign off any emergency change to ensure appropriate segregation of duties. If a user system is affected by the change, a representative of the users should be consulted as part of the decision making process. | The Change Manager to review and amend the Change Management Policy Technical Changes document to ensure consistency and clarity over who can approve a change. | *Agreed action* Policy has been agreed and published. Representative of user of the system consulted where available/possible. No additional actions planned from this recommendation<br><br>*Date Effective:* 27 May 2014<br><br>*Owner:* Head of IT |

# A Internal audit approach

## Approach

Our role as internal auditor to a Public Body is to provide an independent and objective opinion to the Accounting Officer on risk management, control and governance processes, by measuring and evaluating their effectiveness in achieving the organisation's agreed strategic objectives.

Our audit was carried out in accordance with the guidance contained within the Government's Internal Audit Standards (2013) and the Auditing Practices Board's 'Guidance for Internal Auditors'. We also had regard to the Institute of Internal Auditors' guidance on risk based internal auditing (2005). In addition, we comply in all material respects with other Government guidance applicable to Public Bodies and have had regard to the HM Treasury guidelines on effective risk management (the 'Orange Book').

As part of our 2013-14 Audit Plan, we agreed with the Audit Committee and management that we should carry out a review of the ICO's arrangements for managing IT services now delivered by a number of suppliers, to further inform our ongoing understanding of the ICO's key internal control activities.

Our aim in completing this audit was to ensure that the ICO has appropriate arrangements in place to identify, manage and report on risk.

We achieved our audit objectives by:

- meeting with key staff to gain an understanding of the arrangements in place to manage the relationship with suppliers, measure and manage their performance and the quality of delivery of IT services to the ICO;
- identifying the key risks, management controls to mitigate these risks and evaluating the effectiveness of the governance controls over IT service provision; and
- reviewing key documents that support the above processes.

The findings and conclusions from this review will support our annual opinion to the Audit Committee on the adequacy and effectiveness of internal control arrangements.

## Responsibilities

The Information Commissioner acts through his Board of Management and the Information Commissioner's Office ("ICO") discharges his obligations. Therefore references to the Information Commissioner and the ICO in this report relate to one and the same party.

It is the responsibility of the Information Commissioner to ensure that the ICO has adequate and effective risk management, control and governance processes.

HM Treasury's Corporate Governance in Central Government Departments (2011) states that boards of Public Bodies should determine the nature and extent of the significant risks it is willing to take in

achieving its strategic objectives. The Board should therefore maintain sound risk management and internal control systems and should establish formal and transparent arrangements for considering how they should apply the corporate reporting and risk management and internal control principles and for maintaining an appropriate relationship with the organisation's auditors.

Please refer to our letter of engagement for full details of responsibilities and other terms and conditions.

## Scope

Our review involved an assessment of the following risks:

- Service delivery that does not meet ICO requirements.
- Service levels that are unclear or poorly defined lead to misalignment of delivery to user expectations.
- A lack of clear understanding of what is included in the service delivery leading to disputes over ownership or changes that are not appropriately managed that prevent service disruption.
- An inefficient incident management service extends disruption or common faults are not identified to prevent future incidents.

## Additional information

### Client staff

The following staff were consulted as part of this review:

- Daniel Benjamin – Director of Corporate Services
- Dave Wells – Head of IT
- John Rackstraw – IT Service Manager
- Colin Chisholm –Client Service Manager ,Northgate
- Jill Sanderson – Service Delivery Manager, Northgate
- Paul Lee – IT Programme, Group Manager
- Emma Dean – Operation Service Delivery
- Simon Ebbitt – Information Security Manager
- Greer Schick – Online and Internal Communications Manager
- Angela Muston – Contract Manager

### Documents received

The following documents were received during the course of this audit:

- ICO - Quarterly executive IT review - 2013-14 Q3.pptx
- IG - Contracts Manager JD Feb 2013.doc
- IT - job description - Senior IT Service Manager.doc
- IT Service Delivery Group Manager.docx
- IT Strategy for MB 20140127 v2.pptx
- Northgate - Monthly Problem Report Pack - 2013 December.msg
- Quarterly Meeting minutes Jan 2014.docx

**Change Management**

- 140036 - ECAB - Back Out Clearswift Patches.docx
- Change Request Information Email.msg
- Northgate - CHM01 Terms of Reference for Change Management v4.0.pdf
- Northgate - CHM02 High Level Process Design for Change Management v4.0.pdf
- Northgate - CHM03 Account level process design for change management v2..doc
- Northgate Documentation - ICO Requesting Northgate Change.docx
- Northgate documentation - Northgate Requesting ICO Change.docx
- Northgate documentation- NG Requesting ICO Change flowchart.vsd
- Northgate documentation - ICO Requesting NG Change flowchart.vsd

**Contract**

- Appendix to CCN-001 Apps Desktop.docx
- Appendix to CCN-003 Hosting Systems.docx

- Capita Draft Novation Agreement - SCC - ICO - CITS re.Hardware break-fix agreement 12545B.docx
- CCN-001 Change Control Procedure Apps Desktop.docx
- CCN-001 Eduserve IPR Clarification Hosting Systems Management (2).docx
- CCN-002 Addition of Telephony Services.FINAL.Unsigned.docx
- CCN-003 Change Control Procedure Hosting Systems.docx
- CMDB Master - Clients - Desktops Laptops.xlsx
- CMDB Master - Servers, Networks & Printers.xlsx
- Danwood Managed Printed Services Contract.Ts and Cs.FINAL.docx
- Danwood SCHEDULE 2 Services Requirements & Supplier Solution.FINAL.docx
- Danwood SCHEDULE 3.Pricing and Invoicing.FINAL.docx
- FDM Print Services Agreement.FINAL VERSION.docx
- governance meetings
- ICO Contract Management Plan.SCC.Security Contract.v2.Updated 09.07.2013.docx
- Northgate - Application and Desktop management
- Northgate - hosting and Systems management contract
- Sending Draft CCN-002 Various Projects v0 1.msg
- Sending Initial Drafts Appendix 1 to CCN-004 v0 1 Draft CCN-004 Various Projects v0 1.msg
- Sprint II Contract.Software Services - March 2013.FINAL.docx

**Governance Meetings**

- Danwood - Meeting Actions - 20131016.msg
- Danwood - Service review meeting minutes - November 2013.docx
- Northgate - Monthly Service Report -November 2013.docx
- Northgate - monthly service board - December 2013 - agenda.docx
- Northgate - monthly service board - December 2013 - minutes.docx
- Northgate - monthly service board - November 2013 - agenda.docx
- Northgate - Monthly Service Board - November 2013 - minutes.docx
- Northgate - monthly service board - October 13 - minutes.docx
- Northgate - Weekly SRM notes & Incident Report - 20131205.msg
- Northgate - Weekly SRM Notes & Incident Report - 20131211.msg
- Northgate - Weekly SRM Notes & Incident Report - 20140116.msg

Northgate - Weekly SRM Notes & Incident Report - 20140122.msg

**Northgate contracts**

- Apps and Desktop Management.Schedule 2.1 (Service Requirements)FINAL.docx
- Hosting and Systems Management.Schdeule 7.5 (Financial Model) Annex 1.FINAL.xlsx
- Hosting and Systems Management.Schedule 2.1 (Service Requirements)FINAL.docx
- Hosting and Systems Management.Schedule 2.2 (Service Levels)FINAL.docx
- Hosting and Systems Management.Schedule 2.3 (Standards)FINAL.docx
- Hosting and Systems Management.Schedule 2.4 (Continuous Improvement)FINAL.docx
- Hosting and Systems Management.Schedule 2.5(Security Requirements and Security Management Plan)FINAL.docx
- Hosting and Systems Management.Schedule 3 (ICO Responsibilities)FINAL.docx
- Hosting and Systems Management.Schedule 4.1 (Statement of Work)FINAL.docx
- Hosting and Systems Management.Schedule 5.1 (Software)FINAL.docx
- Hosting and Systems Management.Schedule 7.1 (Charges and Invoicing)FINAL.docx
- Hosting and Systems Management.Schedule 7.3 (Value for Money)FINAL.docx
- Hosting and Systems Management.Schedule 7.5 (Financial Model)FINAL.docx
- Hosting and Systems Management.Schedule 8.1 (Governance)FINAL.docx

- Hosting and Systems Management.Schedule 8.2 (Change Control Procedure)FINAL.docx
- Hosting and Systems Management.Schedule 8.3 (Dispute Resolution Procedure)FINAL.docx

**Security**

- ICO - Accreditation Maintenance Plan - v0.1 PROTECT.DOC
- ICO Security Working Group (SWG) - Terms of Reference PROTECT.doc
- Monthly Security Management Board Action Tracker.docx
- Monthly Security Management Board Action Tracker0.docx
- Security Contract SCC Proposal - V4 0 Submitted.docx
- Security Working Group - Security Accreditation Schedule 2013_14.docx
- Simon Ebbitt email.pdf
- SWG - 20130729 - Minutes- PROTECT.doc
- SWG - 20130924 - Minutes- PROTECT.doc
- SWG - 20131218 - Minutes- PROTECT.doc
- SWG - Action Board - PROTECT.doc
- SWG - Action Board - updated 20140107 - PROTECT.doc

## Locations

The following locations were visited during the course of this review:

- The Information Commissioner's Office, Wilmslow

# B Overall assessment and audit issues ratings

## Overall assessment

| Rating | Description |
|---|---|
| **Red** | Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which should be raised with Senior Management and the Audit Committee at the earliest opportunity. |
| **Amber** | Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which require the attention of management to resolve and report on progress in line with current follow up processes. |
| **Green** | We have identified matters which, if resolved, will help management fulfil their responsibility to maintain a robust system of internal control. |

## Audit issue rating

Within each report, every audit issue is given a rating. This is summarised in the table below.

| Rating | Description | Features |
|---|---|---|
| **High** | Findings that are fundamental to the management of risk in the business area, representing a weakness in control that requires the immediate attention of management | • Key control not designed or operating effectively<br>• Potential for fraud identified<br>• Non compliance with key procedures / standards<br>• Non compliance with regulation |
| **Medium** | Important findings that are to be resolved by line management. | • Impact is contained within the department and compensating controls would detect errors<br>• Possibility for fraud exists<br>• Control failures identified but not in key controls<br>• Non compliance with procedures / standards (but not resulting in key control failure) |
| **Low** | Findings that identify non-compliance with established procedures. | • Minor control weakness<br>• Minor non compliance with procedures / standards |
| **Improvement** | Items requiring no action but which may be of interest to management or best practice advice | • Information for department management<br>• Control operating but not necessarily in accordance with best practice |




"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

**grant-thornton.co.uk**